(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10162067 A

(43) Date of publication of application: 19.06.98

(51) Int. Cl G06F 17/60
G06K 17/00

(21) Application number: 08317828

(22) Date of filing: 28.11.96

(71) Applicant: U CARD:KK

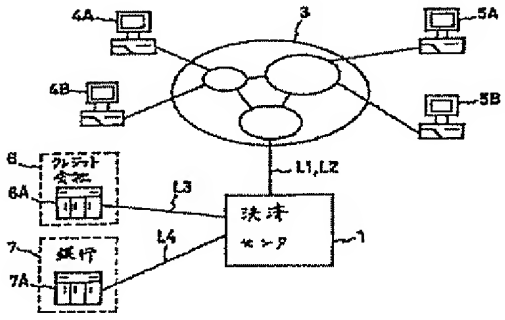
(72) Inventor: OCHIAI YUJI

(54) INFORMATION REGISTERING METHOD UTILIZING NETWORK

(57) Abstract:

PROBLEM TO BE SOLVED: To make the security of held information high by making a terminal transmit a telegraphic message consisting of information and a verification key signing with a signature key generated in a pair with the verification key to a center through a network for registration, and also decodes the signature key and holds it.

SOLUTION: This method is constituted of a settlement center 1, the network 3, general member terminals 4A and 4B, member store terminals 5A and 5B, a center device 6A of a credit company 6, and a center device 7A of a bank 7. A 1st password and a 2nd password for ciphering are inputted and registration contents to the settlement center 1 are inputted. Then, the signature key and a 'kind' for generating the verification key paired with the signature key so as to verify the signature key are inputted. The signature key and verification key corresponding to the inputted 'kind' are generated. The signature key is ciphered with the 2nd password and further ciphered with the 1st password together with history information on the individual and saved in a file.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－162067

(43)公開日　平成10年(1998)６月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３４０Ｚ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
		Ｇ０６Ｆ　15/21	３３０

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

(21)出願番号　特願平8－317828

(22)出願日　平成８年(1996)11月28日

(71)出願人　393007868
株式会社ユーカード
東京都渋谷区元代々木町30－13

(72)発明者　落合　祐二
東京都渋谷区元代々木町30－13　日交元代々木ビル　株式会社ユーカード内

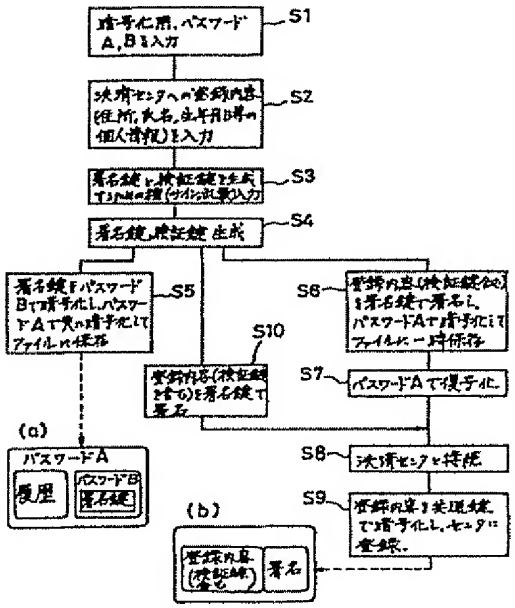
(74)代理人　弁理士　山川　政樹

(54)【発明の名称】　ネットワークを利用した情報の登録方法

(57)【要約】

【課題】　ネットワークを介して個人情報などの情報を登録する場合及び登録した情報について高セキュリティを確保する。

【解決手段】　各端末４，５の利用者は決済センタ１への会員登録時には自身の個人情報と検証鍵とに署名鍵で署名を行ったうえ共通鍵で暗号化して決済センタ１へ送信し、かつ検証鍵と対の上記署名鍵をパスワードＢで暗号化したうえ、パスワードＡでさらに暗号化し自身の端末のファイルに保管する。ここで商品の取引及び決済時等には決済センタへ送信する電文に対し署名鍵により署名を行う一方、決済センタは、電文を受信すると登録してある検証鍵により署名の確認を行う。この結果、商品の決済時等に高セキュリティを確保でき、また他人にパスワードＡが解読されても署名鍵はパスワードＢで更に暗号化されているため署名鍵は本人のみの使用に限定され、電子署名による証拠取引等を行う際に高セキュリティを確保できる。



1

【特許請求の範囲】

【請求項１】　ネットワークを介してセンタと端末とが接続され、端末の情報をネットワークを介して電文としてセンタへ送信し登録するネットワークを利用した情報の登録方法であって、

前記端末は前記情報とこの情報の検証を行うための第１の鍵とからなる前記電文に対し、前記第１の鍵と対に生成される第２の鍵により署名を行ってネットワークを介してセンタへ送信し登録させると共に、前記第２の鍵をパスワードで暗号化して保持することを特徴とするネットワークを利用した情報の登録方法。

【請求項２】　請求項１において、

前記パスワードは第１及び第２のパスワードからなり、

前記端末は前記第１のパスワードで前記第２の鍵を暗号化すると共に、第１のパスワードで暗号化された第２の鍵を第２のパスワードで暗号化して保持することを特徴とするネットワークを利用した情報の登録方法。

【請求項３】　請求項２において、

前記端末は、センタに署名電文を送信する場合は第１のパスワードで暗号化して一時保存すると共に、センタへの送信時にこの署名電文を第１のパスワードで復号化し、かつセンタとの間で一時的に生成される第３の鍵により暗号化して送信し、センタではこの署名電文を受信すると第３の鍵により復号化して登録することを特徴とするネットワークを利用した情報の登録方法。

【請求項４】　請求項１ないし請求項４の何れかの請求項において、

前記情報の登録後に、前記端末から第２の鍵により署名された電文が送信された場合、センタは登録された第１の鍵によりこの署名電文を検証することを特徴とするネットワークを利用した情報の登録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを介して個人情報などの情報を登録する際の情報の登録方法に関する。

【０００２】

【従来の技術】マルチメディア技術の進歩やインターネットの普及により、電子商取引（エレクトロニック・コマース）が現実化しつつある。このようなネットワーク上の決済手段の１つとして、クレジットカードによる決済手段が知られている。

【０００３】

【発明が解決しようとする課題】このような決済システムでは、ネットワークを介して個人情報をセンタに登録しておく必要がある。しかし、こうした決済システムは、インターネット等のネットワークを介在して不特定多数間で電子商取引が行われるため、他人に勝手に個人情報を利用されて不正な取引が行われる恐れがあり、従って暗号技術や本人認証等のセキュリティに関して万全

2

の体制をとることが要望されている。従って本発明は、ネットワークを介して個人情報などの情報を登録する場合及び個人情報を保持する場合に高セキュリティを確保することを目的とする。

【０００４】

【課題を解決するための手段】このような課題を解決するために本発明は、ネットワークを介してセンタと端末とが接続され、端末の情報をネットワークを介して電文としてセンタへ送信して登録する場合、端末は、上記情報とこの情報の検証を行うための第１の鍵（検証鍵）とからなる上記電文に対し、検証鍵と対に生成される第２の鍵（署名鍵）により署名を行ってネットワークを介してセンタへ送信し登録させると共に、端末では署名鍵をパスワードで暗号化して保持するようにした方法である。従って、端末側から個人情報などの情報を電文としてセンタに送信し登録する場合、端末側で個人情報に個人の署名を行ってセンタへ送信すると共に、この署名鍵をパスワードで暗号化して保管するようにしたので、ネットワークを介して登録される個人情報の高セキュリティ性を確保でき、従ってこうした個人情報の第三者による不正使用を的確に防止できる。また、パスワードは個人のみで管理されるため、パスワードの不正使用は本人の不注意によるリークなどによって本人が関与した場合に限られ、システム全体として高いセキュリティを保つことができる。また、上記パスワードを第１及び第２のパスワードから構成し、端末は第１のパスワード（パスワードB）で署名鍵を暗号化すると共に、第１のパスワードで暗号化された署名鍵をさらに第２のパスワード（パスワードA）で暗号化して保持するようにした方法である。従って、第三者に第１のパスワードが解読されたとしても、署名鍵は第２のパスワードでさらに暗号化されているため署名鍵は本人のみの使用に限定され、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。また、端末は、センタへ署名電文を送信する場合は第１のパスワードで暗号化して一時保存すると共に、センタへの送信時点でこの署名電文を第１のパスワードで復号化した後、センタとの間で一時的に生成される共通鍵（第３の鍵）により暗号化して送信し、センタではこの署名電文を共通鍵で復号化したのち登録するようにした方法である。従って、センタに個人情報を登録する場合、より高いセキュリティ性を確保できる。また、上記情報の登録後に、端末から署名鍵により署名された電文が送信された場合、センタは登録された検証鍵によりこの署名電文を検証するようにした方法である。従って、センタでは登録されている検証鍵によりこの電文が真に署名されているか否かを確認でき、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。

【０００５】

【発明の実施の形態】以下、本発明について図面を参照

して説明する。図１は本発明を適用したシステムの構成を示すブロック図である。同図において、１は決済センタ、３はインタネット等のネットワーク、４Ａ，４Ｂは一般会員の所有する端末（以下、一般会員端末）、５Ａ，５Ｂは店舗会員の所有する端末（以下、店舗会員端末）、６Ａはクレジット会社６のセンタ装置、７Ａは銀行７のセンタ装置である。

【０００６】即ち、一般会員端末４Ａ，４Ｂはネットワーク３を介して店舗会員端末５Ａ，５Ｂに接続されていると共に、決済センタ１は専用回線Ｌ１またはＬ２を介してネットワーク３に接続されている。また、決済センタ１はＤＤＸ回線Ｌ３を介してクレジット会社のセンタ装置６Ａに接続され、また専用回線Ｌ４を介して銀行のセンタ装置７Ａに接続されている。

【０００７】ところで、売り手である店舗会員端末５に陳列される商品としては、既存の通信販売形態よって販売される商品（後日配送商品）、その場で販売される文書，ソフトウェア，画像等の商品、及びリアルタイムでコンピュータを運用するゲーム等の商品がある。一方、買い手である一般会員は、例えば決済センタ１の銀行口座等に予め所定額を振り込み、これが決済センタ１により確認されることにより決済センタ１から発行された所定額の価値情報が付与された仮想プリペイドカードを取得している。ここで、店舗会員端末５からネットワーク３を介して提供され端末４に表示される商品が一般会員によって購入されると、決済センタ１ではその一般会員に付与した仮想プリペイドカードの価値情報から購入商品の価格を減じると共に、該当店舗会員に対してその購入商品の対価の支払を行う。

【０００８】次に図２は、決済センタ１の構成を示すブロック図である。同図において、１２はルーター１１により選択された回線を介しネットワーク３との間で各種の情報を授受するWWWサーバ、１３はネットワーク３からの決済センタ１に対する不正なアクセスを防ぐ働きをするセキュリティサーバ、１４はクレジット会社６または銀行７とデータ通信を行う通信サーバ、１５は送信電文（送信データ）の作成，受信電文（受信データ）の解析及びこれらの電文に対し後述の電子署名や署名検証等を行う通信処理サーバ、１６はこれらの処理情報を蓄積するデータベース、１７は決済センタ１においてデータ処理時に発生したエラー情報の出力やログ情報を出力するプリンタである。

【０００９】また、１８は決済サーバであり、決済サーバ１８は、加入者原簿（一般会員原簿），店舗原簿，上記暗号化や電子署名の際に必要となる署名鍵及び検証鍵等の原簿及び処理番号原簿等のデータベース１９に対する記憶管理を行うと共に、通信サーバー１５からの受信データを入力するとデータベース１９の記憶内容に基づき各一般会員に発行した仮想プリペイドカードの決済処理を行い、その処理結果を送信データとして通信処理サーバ１５に与えるものである。また、２０は検索・照会処理，会員の登録処理，返金処理及び統計資料作成処理等を行ってプリンタ２１に出力する照会・統計用サーバである。なお、２３は以上の各部で処理された情報をバックアップするバックアップセンタである。

【００１０】次に図３以降の各図面を用い、本システムの各部の処理動作を具体的に順を追って説明する。まず本システムへの会員の加入処理から説明する。図３は本システムに対する一般会員の加入処理を示す図である。決済センタ１では、ネットワーク３上に常時、一般会員加入申込用の案内画面を送信している（時点①）。ここで、その案内画面を入力したネットワーク３の利用者が端末４から加入要求を行うと（時点②）、決済センタ１では加入画面を作成して端末４へ送る（時点③）。この加入画面を入力した上記利用者が端末４から加入申込を行うと（時点④）、決済センタ１では暗号関数等を用いた入会承認用アプリケーションソフト（以下、ＡＰソフト）が準備してあり、利用者がそのＡＰソフトを端末４へダウンロードする（時点⑤）。その後、決済センタ１では、上記利用者である加入申込者宛に一般会員番号利用規約等を郵送し（時点⑥）、加入申込者がこれを確認して端末４からＡＰソフトを使用し、暗号を用いた会員登録データを送信する（時点⑦）と、決済センタ１ではデータベース１９に会員原簿として登録する。このようにして商品の買い手である一般会員の加入が行われる。

【００１１】次に店舗会員の加入は図４に示す手順で行われる。即ち、決済センタ１からネットワーク３上に送信される店舗会員加盟申込用の案内画面（時点①）に対し、その案内画面を入力したネットワーク３の利用者が端末５から加入要求を行うと（時点②）、決済センタ１では加入画面を作成して端末５へ送る（時点③）。この加入画面を入力した上記利用者が端末５から加入申込を行うと（時点④）、決済センタ１では暗号関数等を用いた加盟承認用ＡＰソフトが準備してあり、利用者がそのＡＰソフトを端末５へダウンロードする（時点⑤）。その後、決済センタ１では、上記利用者である加盟申込者宛に店舗会員番号加盟店約款等を郵送し（時点⑥）、加盟申込者がこれを確認して端末５からＡＰソフトを使用し暗号を用いた店舗登録データを送信する（時点⑦）と、決済センタ１ではデータベース１９に店舗会員原簿として登録する。このようにして商品の売り手である店舗会員の加盟が行われる。

【００１２】こうして各会員が本システムに加入した後、一般会員は、図５に示すように、端末４からネットワーク３を介し後述の電子署名や暗号等を用いた仮想プリペイドカード要求データを決済センタ１へ送信する（時点①）。すると、決済センタ１ではその一般会員からの入金を確認し、電子署名や暗号等を用いた所定額の価値情報の仮想プリペイドカードをその一般会員宛に発行する（時点②）。一般会員は時点②でその仮想プリペ

イドカードをネットワーク３を介して取得する。

【００１３】図１２～図１５は決済センタ１によるこのような仮想プリペイドカードの発行例を示す図である。即ち、図１２の例では、まず一般会員が端末４を用いてプリペイド要求を行う（時点①）。すると決済センタ１ではクレジット会社６に対しこの一般会員に関する与信情報を問い合わせ、与信情報が得られると（時点②）、その一般会員に対して所定額の価値情報を付与した仮想プリペイドカードを発行することで、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点③）。その後、決済センタ１ではクレジット会社６からその所定額を入金し（時点④）、クレジット会社６では、銀行７の上記一般会員の口座から所定額を引き落とす（時点⑤）。

【００１４】次に、図１３の例では、まず一般会員が端末４を用いてプリペイド要求を行う（時点①）と共に、回線を介して自身の口座を有する銀行７１ または郵便局８１に対し、決済センタ１と取引のある銀行７２ または郵便局８２ への所定額の振り込みを指示する（時点②）。すると、銀行７１ または郵便局８１ により、決済センタ１と取引のある銀行７２ または郵便局８２ へ所定額の振り込みが行われる（時点③）。決済センタ１では銀行７２ または郵便局８２ にプリペイド要求を行った上記会員からの入金を確認し、入金が確認されると（時点④）、上記会員宛に所定額の仮想プリペイドカードを発行する。この結果、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点⑤）。

【００１５】次に、図１４の例では、まず一般会員が端末４を用いてプリペイド要求を行う（時点①）と共に、決済センタ１と取引のある銀行７または郵便局８への所定額の振り込みを行う（時点②）。すると、決済センタ１では銀行７または郵便局８にプリペイド要求を行った上記会員からの入金を確認し、入金が確認されると（時点③）、上記会員宛に所定額の仮想プリペイドカードを発行する。この結果、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点④）。

【００１６】次に、図１５の例では、まず一般会員が端末４を用いてプリペイド要求を行う（時点①）と共に、決済センタ１宛に現金書留を郵送する（時点②）。すると、決済センタ１ではプリペイド要求を行った上記会員からの現金書留を受領し入金が確認されると（時点③）、上記会員宛に所定額の仮想プリペイドカードを発行する。この結果、プリペイド要求を行った一般会員はプリペイドカードを取得する（時点④）。

【００１７】こうして一般会員は価値情報が付与された仮想プリペイドカードを取得すると、図６に示すように、端末４を操作し、店舗会員端末５からネットワーク３を介して提供され端末４に表示される各商品のうち、購入したい何れかの商品を選択し（時点①）、受発注処理を完了させて（時点②）、その代金精算を決済センタ

１へ指示する（時点③）。すると、一般会員端末４と店舗会員端末５との間で以下に示すような取引処理が開始される。

【００１８】即ち、図７に示すように、この場合まず端末４から電子署名および暗号が施された取引番号等の要求情報（支払指示）がネットワーク３を介して決済センタ１へ送られる（時点①）。すると、決済センタ１ではこの取引番号要求を行った会員が一般会員であることを確認のうえ、その一般会員の残高認証を行い（時点②）、ネットワーク３を介して端末５に対し電子署名および暗号を施した取引番号等の要求情報（支払通知）を送信する（時点③）と共に、端末４に対して新残高を通知する（時点④）。この結果、一般会員及び店舗会員の決済が完了する。

【００１９】このようにして商品の売買及び決済処理が行われた後、店舗会員端末５からネットワーク３を介して一般会員端末４宛に販売商品の受け渡しが行われる（図８）。なお、ここでネットワーク３を介して配送される商品の類としては、上述した文書，ソフトウェア及び画像等の商品があり、既存の通信販売形態の商品は、後日配送される。そして販売商品の配送が行われた後、図９に示すように、店舗会員端末５から決済センタ１に対してその販売商品に相当する代金の支払請求が送信される（時点①）。すると、決済センタ１では、銀行７の該当店舗会員の口座に該代金相当額を振り込む（時点②）。

【００２０】このように本システムは、商品の買い手はクレジットカードまたはホームバンキングの手段で決済センタ１から仮想プリペイドカードを購入し、電子商取引を行う一方、商品の売り手は電子商取引にあたって決済センタ１を介し買い手の仮想残高を商品代金分だけ減額すると共に、決済センタ１に対して代金請求を行い支払を受けるようにしたものである。

【００２１】図１０は、本発明の要部動作を示すもので、各端末４，５から決済センタ１に対し会員登録を行う場合の各端末４，５の動作状況を示す流れ図であり、図１０に示すような各ステップを踏むことによりシステムとして高いセキュリティ性を確保できる。即ち、ステップＳ１では、まず２つの暗号化用パスワードＡ（第１のパスワード，及びパスワードＢ（第２のパスワード）を入力する。続いてステップＳ２では、決済センタ１への登録内容の入力操作を行う。この登録内容としては、会員個人の住所，氏名，生年月日等の個人情報が含まれる。そして続いてステップＳ３では後述の署名鍵（秘密鍵；印鑑に相当）及びこの署名鍵を検証する為の署名鍵と対になる検証鍵（公開鍵）を生成するための「種」を入力する。ここでこの「種」を入力する場合は、例えば会員個人の自筆によるサインが端末４の図示しないキーボードから入力されるか、或いは、端末４内で乱数を用いて自動的に入力される。すると、ステップＳ４では入

力された「種」に応じた署名鍵及び検証鍵が生成される。ここで、署名鍵及び検証鍵を生成する場合は、署名鍵の関数が検証鍵となるように生成される。即ち、一例として署名鍵をｐ，ｑとした場合、検証鍵ｎは、ｎ＝ｐ２×ｑとなるように生成される。

【００２２】生成された署名鍵は各端末４，５においてそれぞれ図示しないファイルに保存される。ここで署名鍵をファイルに保存する場合は、ステップＳ５で署名鍵をパスワードＢで暗号化し、これをさらにパスワードＡにより、その個人の履歴情報（即ち、この場合は個人の商品購入履歴情報）とともに暗号化してファイルに保存する。この結果、署名鍵は図１０（ａ）に示すような階層構造でファイルに保管される。従って、第三者にパスワードＡが解読されたとしても、第三者はそのパスワードＡに該当する個人の商品購入履歴情報等を端末の図示しない表示部に表示できるのみであり、署名鍵はパスワードＢでさらに暗号化されているために第三者による商品購入等の決済を伴う行為（署名が必要なサービス）に使用されることはなく、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。

【００２３】次に決済センタ１に対して上述の入力内容を登録する場合は、次のような２通りの方法がある。まず、第１の方法は、ステップＳ２で入力した内容とステップＳ４で生成された検証鍵に対しステップＳ６で署名鍵により署名し、これをパスワードＡにより暗号化してファイルに一旦保存する。次いでステップＳ７でパスワードＡによる暗号を解いた（復号化）後、ステップＳ８で決済センタ１と回線接続を行う。そしてその後、ステップＳ９でその登録内容を決済センタ１との伝送の際に一時的に生成される共通鍵（暗号鍵）により暗号化し、決済センタ１へ伝送する。決済センタ１ではこの電文を上記共通鍵により復号化して登録する。次に第２の方法は、ステップＳ２で入力した内容とステップＳ４で生成された検証鍵に対しステップＳ１０で署名鍵により署名したのち、ステップＳ８で決済センタ１と回線接続を行う。そしてその後、ステップＳ９でその登録内容を決済センタ１との伝送の際に一時的に生成される共通鍵（暗号鍵）により暗号化し、決済センタ１へ伝送する。決済センタ１ではこの電文を上記共通鍵により復号化して登録する。

【００２４】このようにして一般会員や店舗会員の個人データが図１０（ｂ）に示すような形態で決済センタ１に登録される。その後、決済センタ１では各端末から署名鍵により署名された電文が送られてきた場合、後述するようにその署名鍵と対の検証鍵により、その電文が真に電子署名されているか否かを検証するため、商品取引において信頼性の高いシステムを実現できる。

【００２５】図１１は、こうして決済センタ１に登録された一般会員の端末４が電子商取引を行う場合の動作を示す流れ図である。即ち、決済センタ１と未接続状態（オフライン状態）にある一般会員端末４においてステップＳ１１でパスワードＡの入力操作が行われると、その一般会員端末４に保存された過去の取引データ（即ち、買い物履歴データ；商品購入履歴情報）をステップＳ１２で図１１（ａ）に示す表示データとして端末４の図示しない表示部に表示させる。なお、図１１（ａ）において、ｙｙ，ｍｍ，ｄｄは各々、年，月，日を示す。

【００２６】続いて上記一般会員端末４においてステップＳ１３でパスワードＢの入力操作が行われると、この会員端末４では、決済センタ１に送信される電文（即ち、例えば図７の説明で述べた取引番号要求データ）に署名を行うための署名鍵が取り出されたものと判断し、ステップＳ１４において決済センタ１との間で署名が必要なサービスへ移行する。即ち、上述のパスワードＢの入力により署名鍵が取り出され決済センタ１と回線接続が行われた後、上記の電文がその署名鍵で署名されこの署名電文がその一般会員端末４から送信されたとすると、決済センタ１ではこの電文を受信し、会員登録時に登録されている検証鍵によりこの受信電文を解読し確認する。そして確認がＯＫになると、その一般会員の残高認証を行った後に店舗会員端末５に対し電子署名および暗号を施した支払通知を送信すると共に、その一般会員端末４に対し新残高を通知する。

【００２７】このように、決済時には必ず使用される署名鍵をパスワードＡ，Ｂにより暗号化するため、パスワードＡが解読され署名鍵の在処が第三者に分かってしまったような場合でも、第三者は署名鍵を取り出すことができず、従って第三者による署名鍵の使用を防止することができる。即ち、この場合、第三者はこの署名鍵の持ち主の例えば買い物履歴等が閲覧できるだけであって、署名が必要な決済サービスへの移行を阻止できる。また、第三者が署名鍵を偶然入手したとしても、署名鍵を利用し難いという効果も期待でき、またパスワードＢを偶然入手したとしてもパスワードＡを入手しない限り署名鍵を取り出せないことから、パスワードＢの利用を阻止する効果も期待できる。

【００２８】さらに、署名鍵と検証鍵とを対に設け、署名鍵は各端末で管理し、検証鍵は決済センタ１で一括して管理することにより、署名鍵が第三者の手に渡ってしまった場合でも決済が必要な商取引時には第三者は必ず決済センタ１を利用して検証鍵により電文を解読させなければならないため、署名鍵の暗号化の度合いを弱めることもできる。従って、署名鍵を暗号化する場合パスワードＡのみで行い、パスワードＢを不要にすることができる。

【００２９】

【発明の効果】以上説明したように本発明によれば、ネットワークを介してセンタと端末とが接続され、端末側から個人情報などの情報を電文としてセンタに送信し登録する場合、端末側で個人情報に個人の署名を行ってセ

9

ンタへ送信すると共に、この署名鍵をパスワードで暗号化して保管するようにしたので、ネットワークを介して登録される個人情報の高セキュリティ性を確保でき、従ってこうした個人情報の第三者による不正使用を的確に防止できる。また、パスワードは個人のみで管理されるため、パスワードの不正使用は本人の不注意によるリークなどによって本人が関与した場合に限られ、システム全体として高いセキュリティを保つことができる。また、上記パスワードを第１及び第２のパスワードから構成し、端末は第１のパスワードで署名鍵を暗号化すると共に、第１のパスワードで暗号化された署名鍵をさらに第２のパスワードで暗号化して保持するようにしたので、第三者に第１のパスワードが解読されたとしても、署名鍵は第２のパスワードでさらに暗号化されているため署名鍵は本人のみの使用に限定され、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。また、端末は、センタに署名電文を送信する場合は第１のパスワードで暗号化して一時保存すると共に、センタへの送信時点でこの署名電文を第１のパスワードで復号化した後、共通鍵で暗号化して送信し、センタではこの署名電文を共通鍵で復号化して登録するようにしたので、センタに個人情報を登録する場合、より高いセキュリティ性を確保できる。また、上記個人情報の登録後に、端末から署名鍵により署名された電文が送信された場合、センタは登録された検証鍵によりこの署名電文を検証するようにしたので、センタではこの電文が真に署名されているか否かを確認でき、この結果、電子署名による証拠取引を行う場合に高セキュリティ性を確保できる。

【図面の簡単な説明】

【図１】　本発明のシステムの構成を示すブロック図である。

10

【図２】　上記システムを構成する決済センタのブロック図である。

【図３】　一般会員の登録動作を示す図である。

【図４】　店舗会員の登録動作を示す図である。

【図５】　一般会員端末を介する仮想プリペイドカード取得動作を示す図である。

【図６】　一般会員端末を介する購入商品の選択動作及び受発注動作を示す図である。

【図７】　商品取引時の決済動作を示す図である。

【図８】　商品取引時の商品引き渡し状況を示す図である。

【図９】　商品取引時の決済センタの支払動作を示す図である。

【図１０】　各端末が決済センタに対し会員登録を行う場合の動作状況を示す流れ図である。

【図１１】　一般会員端末が電子商取引を行う場合の動作を示す流れ図である。

【図１２】　仮想プリペイドカード取得の第１の例を示す図である。

【図１３】　仮想プリペイドカード取得の第２の例を示す図である。

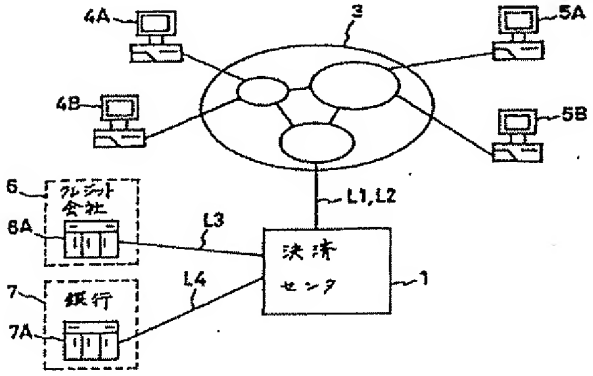
【図１４】　仮想プリペイドカード取得の第３の例を示す図である。

【図１５】　仮想プリペイドカード取得の第４の例を示す図である。

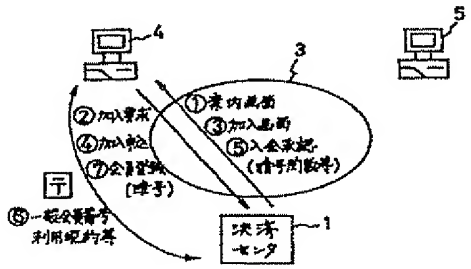
【符号の説明】

１…決済センタ、３…ネットワーク、４，４Ａ，４Ｂ…一般会員端末、５，５Ａ，５Ｂ…店舗会員端末、６…クレジット会社、７，７１，７２…銀行、８，８１，８２…郵便局、６Ａ，７Ａ，８Ａ…センタ装置、１１，２２…ルーター、１２～１５，１７，１８，２０…サーバー、２３…バックアップセンタ。

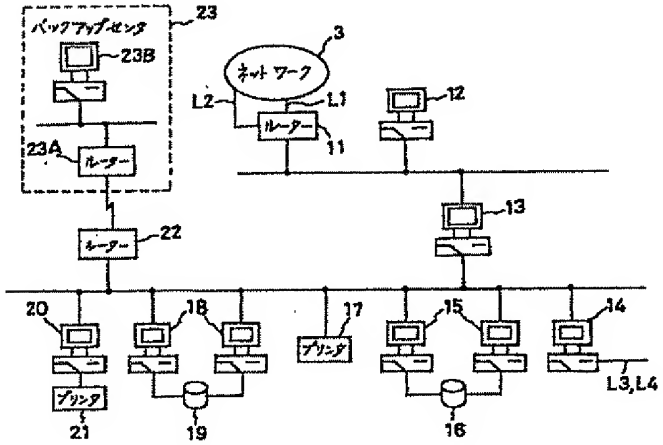
【図１】



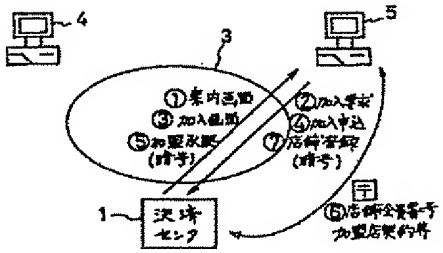
【図３】



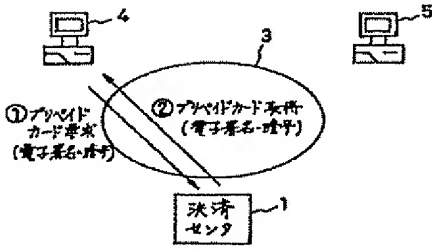
【図２】



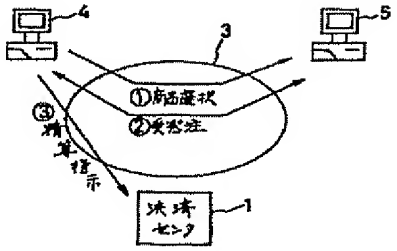
【図４】



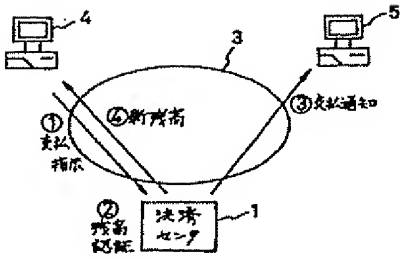
【図５】



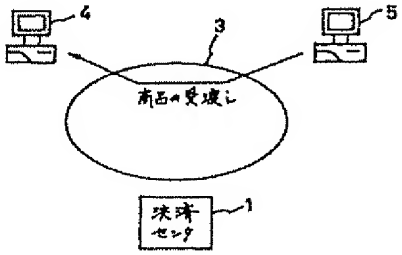
【図６】



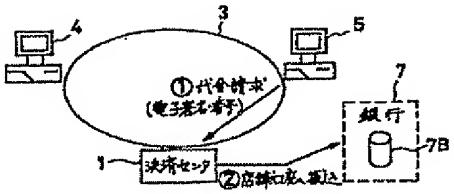
【図７】



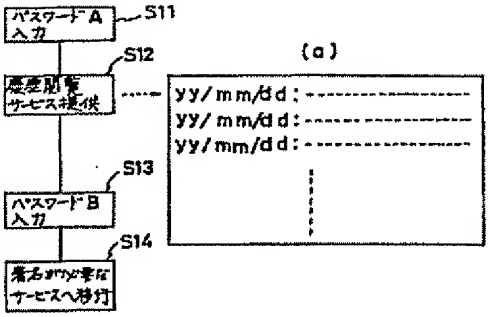
【図８】



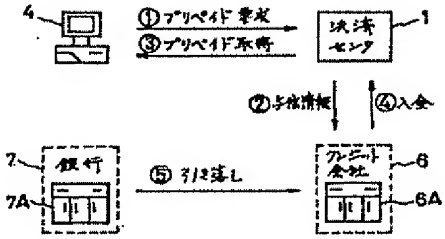
【図９】



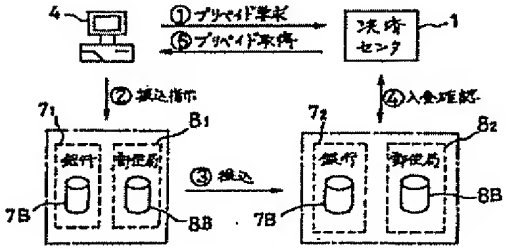
【図１１】



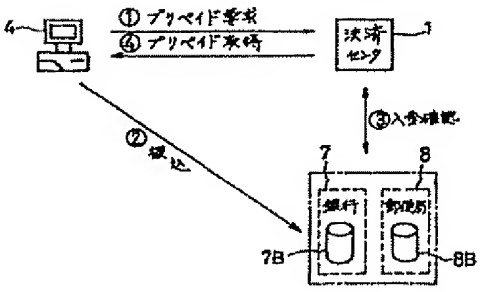
【図１２】



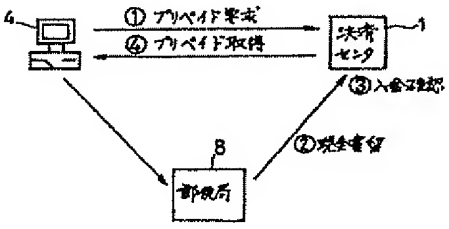
【図１３】



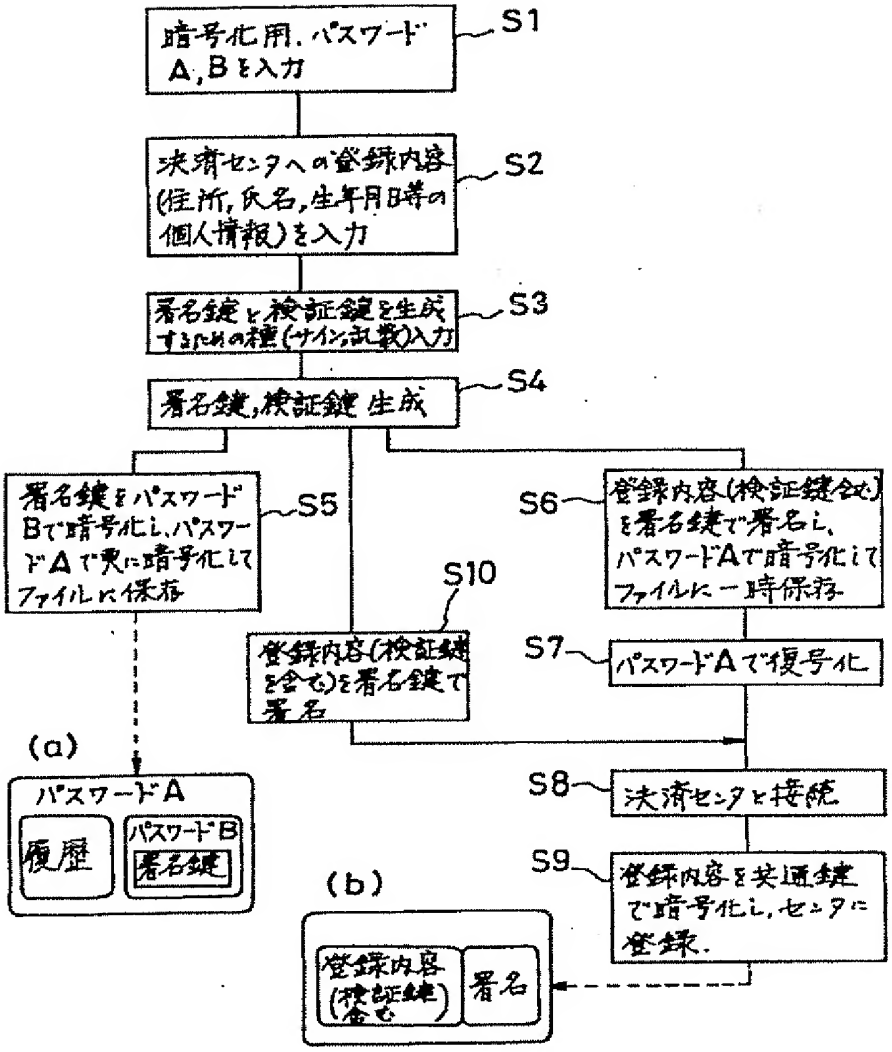
【図１４】



【図１５】



【図１０】


暗号化用．パスワードA，Bを入力
S1
決済センタへの登録内容(住所，氏名，生年月日等の個人情報)を入力
S2
署名鍵と検証鍵を生成するための種(サイン，乱数)入力
S3
署名鍵，検証鍵 生成
S4
署名鍵をパスワードBで暗号化し，パスワードAで更に暗号化してファイルに保存
S5
登録内容(検証鍵含む)を署名鍵で署名し，パスワードAで暗号化してファイルに一時保存
S6
S10
登録内容(検証鍵を含む)を署名鍵で署名
S7
パスワードAで復号化
(a)
パスワードA
履歴
パスワードB
署名鍵
S8
決済センタと接続
S9
登録内容を共通鍵で暗号化し，センタに登録．
(b)
登録内容(検証鍵含む)
署名

JAPANESE [JP,10-162067,A]

CLAIMS DETAILED DESCRIPTION TECHNICAL FIELD PRIOR ART EFFECT OF THE INVENTION TECHNICAL PROBLEM MEANS DESCRIPTION OF DRAWINGS DRAWINGS

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]It is a registration method of information using a network which a center and a terminal are connected via a network, and transmits to a center as wording of a telegram, and registers information on a terminal via a network, Said terminal signs with said 1st key and the 2nd key generated by pair to said wording of a telegram which consists of the 1st key for performing verification of said information and this information, and it transmits to a center, and make it register via a network, and. A registration method of information using a network enciphering and holding said 2nd key with a password.
[Claim 2]In claim 1, said password consists of the 1st and 2nd passwords, and said terminal enciphers said 2nd key with said 1st password, and. A registration method of information using a network enciphering and holding the 2nd key enciphered with the 1st password with the 2nd password.
[Claim 3]In claim 2, when transmitting signature wording of a telegram to a center, encipher with the 1st password, save said terminal temporarily, and. A registration method of information using a network decrypting with the 3rd key and registering if this signature wording of a telegram is decrypted with the 1st password at the time of transmission in the center, and it enciphers with the 3rd key generated temporarily, it transmits between centers and this signature wording of a telegram is received in the center.
[Claim 4]A registration method of information using a network when wording of a telegram signed with the 2nd key from said terminal after registration of said information is transmitted in which claim of claim 1 thru/or claim 4, wherein a center verifies this signature wording of a telegram with the 1st registered key.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the registration method of the information at the time of registering information, including personal information etc., via a network.
[0002]
[Description of the Prior Art]Electronic commerce technology (electronic commerce) is being realized by progress of multimedia art or the spread of the Internet. The payment system by a credit card is known as one of the payment systems on such a network.
[0003]
[Problem(s) to be Solved by the Invention]It is necessary to register personal information into a center via a network in such a settlement system. However, since such a settlement system intervenes networks, such as the Internet, and electronic commerce technology is performed between many and unspecified persons, there is a possibility that personal information may be freely used for others and unjust dealings may be conducted to them -- therefore, encoding technology and the person himself/herself -- it is requested that thoroughgoing organization is taken about security, such as attestation. Therefore, an object of this invention is to secure high security, when registering information, including personal information etc., via a network, and when holding personal information.
[0004]
[Means for Solving the Problem]In order to solve such a technical problem, a center and a terminal are connected to this invention via a network, When transmitting to a center as wording of a telegram and registering information on a terminal via a network, a terminal, Sign with verification keys and the 2nd key (signature key) generated by pair to the above-mentioned wording of a telegram which consists of the 1st key (verification keys) for performing verification of the above-mentioned information and this information, transmit to a center, and make it register via a network, and. It is the method which enciphers with a password and held a signature key at a terminal. Therefore, when transmitting and registering with a center from the terminal side by making information, including personal information etc., into wording of a telegram, sign personal information in an individual by the terminal side, transmit to a center, and. Since it enciphers with a password and was made to keep this signature key, the high security nature of personal information registered via a network can be secured, therefore an unauthorized use by a third party of such personal information can be prevented exactly. Since a password is managed only individually, an unauthorized use of a password is restricted when the person himself/herself involves by leak by inattention of the person himself/herself, etc., and it can maintain security high as the whole system. Constituting the above-mentioned password from the 1st and 2nd passwords, a terminal enciphers a signature key with the 1st password (password B), and it is the method which enciphers with the 2nd password (password A) further, and held a signature key enciphered with the 1st password. Therefore, even if the 1st password is decoded by third party, since a signature key is further enciphered with the 2nd password, when a signature key is limited to use of only the person himself/herself and it, as a result, conducts dealings of evidence by an electronic signature, high security nature can be secured.

When transmitting signature wording of a telegram to a center, encipher with the 1st password, save a terminal temporarily, and. It is at the transmitting-in center time, and after decrypting this signature wording of a telegram with the 1st password, it is the method registered after having enciphered with a common key (the 3rd key) generated temporarily, transmitting between centers and decryptlng this signature wording of a telegram with a common key in the center. Therefore, when registering personal information into a center, higher security nature can be secured. When wording of a telegram signed by a signature key from a terminal is transmitted after registration of the above-mentioned information, a center is the method which verified this signature wording of a telegram by registered verification keys. Therefore, in the center, when it can be checked whether this wording of a telegram is signed truly by verification keys registered and, as a result, conducts dealings of evidence by an electronic signature, high security nature can be secured.

[0005]

[Embodiment of the Invention]Hereafter, this invention is explained with reference to drawings. Drawing 1 is a block diagram showing the composition of the system which applied this invention. In the figure, the center apparatus of the credit company 6 and 7A of networks, such as the Internet, the terminal (the following, common member's terminal) which a settlement center owns 1, 4A owns 3, and, as for 4B, a general member owns, the terminal (henceforth, store member's terminal) which, as for 5A and 5B, a store member owns, and 6A are the center apparatus of the bank 7.

[0006]That is, the common member's terminals 4A and 4B are connected to the store member's terminals 5A and 5B via the network 3, and the settlement center 1 is connected to the network 3 via the dedicated line L1 or L2. It is connected to the center apparatus 6A of a credit company via the DDX circuit L3, and the settlement center 1 is connected to the center apparatus 7A of a bank via the dedicated line L4.

[0007]By the way, there are goods (later delivered goods) which are the existing mail order gestalten and are sold as goods displayed by the store member's terminal 5 which is a seller, goods, such as a document sold on that spot, software, and a picture, and goods, such as a game which employs a computer in real time. On the other hand, the general member who is a buyer transferred specified amount, for example to the bank account of the settlement center 1, etc. beforehand, and when this is checked by the settlement center 1, he acquires the virtual prepaid card in which the value information of the specified amount published from the settlement center 1 was given. If the goods which are provided via the network 3 from the store member's terminal 5, and are displayed on the terminal 4 here are purchased by the general member, In the settlement center 1, the price of purchasing commodities is subtracted from the value information of the virtual prepaid card given to the general member, and payment of the remuneration of the purchasing commodity is made to an applicable store member.

[0008]Next, drawing 2 is a block diagram showing the composition of the settlement center 1. The WWW server with which 12 delivers between the networks 3 and receives various kinds of information via the circuit selected with the router 11 in the figure, The security server which serves to prevent unjust access of as opposed to the settlement center 1 from the network 3 in 13, The communications server with which 14 performs the credit company 6 or the bank 7, and data communications, The communication processing server with which 15 performs a below-mentioned electronic signature, signature verification, etc. to creation of transmitted wording of a telegram (send data), the analyses of a received message (received data), and these wording of a telegram, The database with which 16 accumulates these processing information, and 17 are printers which output the output and log information of the error information generated in the settlement center 1 at the time of data processing.

[0009]18 is a settling server and the settling server 18, Perform storage and file management to the databases 19, such as registers, such as a member register (general member register), a store register, a signature key that is needed in the case of the above-mentioned encryption or an electronic signature, and verification keys, and a treating number register, and. If the received data from the communications server 15 are inputted, settlement processing of the virtual prepaid card published to each general member based on the memory content of the database

19 will be performed, and it gives the communication processing server 15 by using the processing result as send data. 20 is a server for reference / statistics which performs search and inquiry processing, a member's registration processing, refund processing, statistical-materials creation processing, etc., and is outputted to the printer 21. 23 is a backup center which backs up the information processed in the above each part.

[0010]Next, order is concretely explained for the processing operation of each part of this system later on using each drawing after drawing 3. It explains from the subscription processing of the member to this system first. Drawing 3 is a figure showing a general member's subscription processing to this system. In the settlement center 1, the initial screen format for a general member subscription application is always transmitted on the network 3 (time **). Here, if the user of the network 3 who inputted the initial screen format performs a subscription request from the terminal 4 (time **), in the settlement center 1, a subscription screen will be created and it will send to the terminal 4 (time **). If the above-mentioned user who inputted this subscription screen makes a subscription application from the terminal 4 (time **), in the settlement center 1, the application software for admission recognition (henceforth, AP software) which used the code function etc. will be prepared, and a user will download that AP software to the terminal 4 (time **). Then, general membership number use agreement etc. are mailed to the subscription proposer who is the above-mentioned user in the settlement center 1 (time **), membership registration data a subscription proposer checks this, use AP software from the terminal 4, and using the code -- transmitting (time **) -- in the settlement center 1, it registers with the database 19 as a member register. Thus, subscription of the general member who is a buyer of goods is performed.

[0011]Next, a store member's subscription is performed in the procedure shown in drawing 4. That is, if the user of the network 3 who inputted the initial screen format from the settlement center 1 to the initial screen format for a store member affiliation application (time **) transmitted on the network 3 performs a subscription request from the terminal 5 (time **), in the settlement center 1, a subscription screen will be created and it will send to the terminal 5 (time **). If the above-mentioned user who inputted this subscription screen makes a subscription application from the terminal 5 (time **), in the settlement center 1, AP software for affiliation recognition which used the code function etc. will be prepared, and a user will download that AP software to the terminal 5 (time **). Then, in the settlement center 1, a store membership number member's store article etc. are mailed to the affiliation proposer who is the above-mentioned user (time **), store registration data an affiliation proposer checks this and using the code using the terminal 5 to AP software -- transmitting (time **) -- in the settlement center 1, it registers with the database 19 as a store member register. Thus, affiliation of the store member who is a seller of goods is performed.

[0012]In this way, after each member joins this system, a general member transmits the virtual prepaid card requested data using a below-mentioned electronic signature, a code, etc. to the settlement center 1 via the network 3 from the terminal 4, as shown in drawing 5 (time **). Then, in the settlement center 1, the payment from the general member is checked and the virtual prepaid card of the value information of the specified amount using an electronic signature, a code, etc. is published to the addressing to a general member (time **). A general member acquires the virtual prepaid card via the network 3 by time **.

[0013]Drawing 12 - drawing 15 are the figures showing the example of issue of such a virtual prepaid card by the settlement center 1. That is, in the example of drawing 12, a general member performs a prepaid demand using the terminal 4 first (time **). By then, the thing for which the virtual prepaid card which gave the value information of specified amount to that general member will be published if the credit data about this general member are asked to the credit company 6 in the settlement center 1 and credit data are acquired (time **). The general member who performed the prepaid demand acquires a prepaid card (time **). Then, in the settlement center 1, the specified amount is paid in from the credit company 6 (time **), and specified amount is pulled down from the account of the above-mentioned general member of the bank 7 in the credit company 6 (time **).

[0014]next -- in the example of drawing 13, a general member uses the terminal 4 first -- a

prepaid demand — carrying out (time **) — transfer of the specified amount to the bank 72 or the post office 82 with the settlement center 1 and dealings is directed to the bank 71 or the post office 81 which has an own account via a circuit (time **). Then, transfer of specified amount is performed by the bank 71 or the post office 81 at the bank 72 or the post office 82 with the settlement center 1 and dealings (time **). In the settlement center 1, if the payment from the above-mentioned member who gave the prepaid demand to the bank 72 or the post office 82 is checked and payment is checked (time **), the virtual prepaid card of specified amount will be published to the above-mentioned addressing to a member. As a result, the general member who performed the prepaid demand acquires a prepaid card (time **).

[0015]next — in the example of drawing 14, a general member uses the terminal 4 first — a prepaid demand — carrying out (time **) — the specified amount to the bank 7 or the post office 8 with the settlement center 1 and dealings is transferred (time **). Then, in the settlement center 1, if the payment from the above-mentioned member who gave the prepaid demand to the bank 7 or the post office 8 is checked and payment is checked (time **), the virtual prepaid card of specified amount will be published to the above-mentioned addressing to a member. As a result, the general member who performed the prepaid demand acquires a prepaid card (time **).

[0016]next — in the example of drawing 15, a general member uses the terminal 4 first — a prepaid demand — carrying out (time **) — registered mail is mailed to the settlement center 1 (time **). Then, in the settlement center 1, if the registered mail from the above-mentioned member who performed the prepaid demand is received and payment is checked (time **), the virtual prepaid card of specified amount will be published to the above-mentioned addressing to a member. As a result, the general member who performed the prepaid demand acquires a prepaid card (time **).

[0017]In this way, if the virtual prepaid card in which value information was given is acquired, as shown in drawing 6, a general member, Operate the terminal 4, choose which goods to purchase among each goods which are provided via the network 3 from the store member's terminal 5, and are displayed on the terminal 4 (time **), order-taking-and-order-placement processing is made to complete (time **), and the price balancing account is directed to the settlement center 1 (time **). Then, processing of transactions as shown below between the common member's terminal 4 and the store member's terminal 5 is started.

[0018]That is, as shown in drawing 7, the demand information (payment indication), including a transaction number etc., that the electronic signature and the code were given is first sent to the settlement center 1 via the network 3 from the terminal 4 in this case (time **). In then, the settlement center 1 That member who performed this transaction number demand is general member check-top, demand information (advice of payment), including the transaction number etc. which performed the general member's balance attestation (time **), and gave the electronic signature and the code to the terminal 5 via the network 3, — transmitting (time **) — — new remainder is notified to the terminal 4 (time **). As a result, settlement of accounts of a general member and a store member is completed.

[0019]Thus, after dealing of goods and settlement processing are performed, delivery of selling merchandise is performed to the common member's terminal 4 via the network 3 from the store member's terminal 5 (drawing 8). As a class of the goods delivered via the network 3 here, there are goods mentioned above, such as a document, software, and a picture, and the product of the existing mail order gestalt is delivered later. And after delivery of selling merchandise is performed, as shown in drawing 9, the application for payment of the price which is equivalent to the selling merchandise from the store member's terminal 5 to the settlement center 1 is transmitted (time **). Then, in the settlement center 1, this price amount equivalent is transferred to the account of the applicable store member of the bank 7 (time **).

[0020]Thus, as for this system, the buyer of goods purchases a virtual prepaid card from the settlement center 1 by the means of a credit card or a home banking, The seller of goods reduces a buyer's virtual balance by a commodity price via the settlement center 1 in electronic commerce technology, and performs invoicing to the settlement center 1, and used to be made to receive payment, while performing electronic commerce technology.

[0021]Drawing 10 is a flow chart in which showing important section operation of this invention, and showing the operation situation of each terminals 4 and 5 in the case of holding membership registration from each terminals 4 and 5 to the settlement center 1, and can secure security nature high as a system by stepping on each step as shown in drawing 10. That is, at Step S1, they are the two passwords A for encryption (the 1st password and the password B (the 2nd password) are entered.) first. Then, in Step S2, alter operation of the contents of registration to the settlement center 1 is performed. As these contents of registration, personal information, such as a member individual's address, a name, and a date of birth, is included. And the "kind" for generating the verification keys (public key) which become a signature key for verifying a below-mentioned signature key (secret key; equivalent to a seal) and this signature key at Step S3 continuously and a pair is inputted. When inputting this "kind" here, the sign by a member individual's autograph is inputted from the keyboard which the terminal 4 does not illustrate, for example, or it is automatically inputted using a random number within the terminal 4. Then, in step S4, the signature key and verification keys according to the inputted "kind" are generated. Here, when generating a signature key and verification keys, it is generated so that the function of a signature key may serve as verification keys. That is, when a signature key is set to p and q as an example, the verification keys n are generated so that it may be set to $n=p^2xq$.
[0022]The generated signature key is saved at the file which is not illustrated in each terminals 4 and 5, respectively. When saving a signature key here at a file, a signature key is enciphered with the password B at Step S5, it enciphers with the password A further with that individual's hysteresis information (namely, in this case individual merchandise purchase hysteresis information), and this is saved at a file. As a result, a signature key is kept by the file by a layered structure as shown in drawing 10 (a). Therefore, it is only that the third party can display the merchandise purchase hysteresis information of the individual applicable to the password A, etc. on the indicator which a terminal does not illustrate even if the password A is decoded by the third party, The signature key can secure high security nature, when it is not used for the act (service to be signed) accompanied by settlement of the merchandise purchase by a third party, etc. and, as a result, conducts the dealings of evidence by an electronic signature, since it is further enciphered with the password B.
[0023]Next, when registering an above-mentioned entry content to the settlement center 1, there are two kinds of following methods. First, the 1st method signs with a signature key at Step S6 to the contents inputted at Step S2, and the verification keys generated by step S4, enciphers this with the password A, and once saves it at a file. Subsequently, after solving a code with the password A at Step S7 (decryption), the settlement center 1 and a line connection are performed at Step S8. And after that, it enciphers with the common key (encryption key) temporarily generated by step S9 in the case of transmission of the contents of registration with the settlement center 1, and transmits to the settlement center 1. In the settlement center 1, this wording of a telegram is decrypted with the above-mentioned common key, and is registered. Next, the 2nd method performs the settlement center 1 and a line connection at Step S8, after signing with a signature key at Step S10 to the contents inputted at Step S2, and the verification keys generated by step S4. And after that, it enciphers with the common key (encryption key) temporarily generated by step S9 in the case of transmission of the contents of registration with the settlement center 1, and transmits to the settlement center 1. In the settlement center 1, this wording of a telegram is decrypted with the above-mentioned common key, and is registered.
[0024]Thus, it registers with the settlement center 1 with a gestalt as the personal data of a general member or a store member show to drawing 10 (b). Then, since it verifies whether the electronic signature of the wording of a telegram is carried out truly by the signature key and a pair of verification keys so that it may mention later when the wording of a telegram signed by the signature key from each terminal has been sent, in a commodity transaction, a reliable system is realizable in the settlement center 1.
[0025]Drawing 11 is a flow chart showing operation in case a general member's terminal 4 registered into the settlement center 1 in this way performs electronic commerce technology.

Namely, if alter operation of the password A is performed at Step S11 in the settlement center 1 and the common member's terminal 4 in a non-connected state (offline state), The past transaction data (namely, shopping historical data; merchandise purchase hysteresis information) saved at the common member's terminal 4 is displayed on the indicator which the terminal 4 does not illustrate as an indicative data shown in drawing 11 (a) at Step S12. In drawing 11 (a), yy, mm, and dd show a year, the moon, and a day respectively.
[0026]Then, when alter operation of the password B is performed at Step S13 in the above-mentioned general member's terminal 4, in this member's terminal 4. It is judged as that from which the signature key for signing the wording of a telegram (namely, transaction number requested data described, for example by explanation of drawing 7) transmitted to the settlement center 1 was taken out, and a signature shifts to required service between the settlement centers 1 in Step S14. Namely, after a signature key is taken out by the input of the above-mentioned password B and the settlement center 1 and a line connection are performed, supposing the above-mentioned wording of a telegram is signed with that signature key and this signature wording of a telegram is transmitted from that common member's terminal 4, In the settlement center 1, this wording of a telegram is received, and this received message is decoded by the verification keys registered at the time of membership registration, and it checks. And if a check is set to O.K., after performing the general member's balance attestation, the advice of payment which gave the electronic signature and the code to the store member's terminal 5 will be transmitted, and new remainder is notified to the common member's terminal 4.

[0027]Thus, in order to encipher the signature key certainly used with the passwords A and B at the clearing time, Even when the password A was decoded and a third party understands the whereabouts of a signature key, the third party cannot take out a signature key, therefore can prevent use of the signature key by a third party. That is, in this case, the third party can only peruse for example, the shopping history of the owner of this signature key, etc., and can prevent the shift to account settlement services to be signed. Since a signature key cannot be taken out unless the password A comes to hand, even if it can also expect the effect of being hard to use a signature key and the password B comes to hand by chance, even if a third party obtains a signature key by chance, the effect which prevents use of the password B is also expectable.
[0028]By providing a signature key and verification keys in a pair, managing a signature key at each terminal, putting verification keys in block in the settlement center 1, and managing, Since the third party has to make wording of a telegram certainly decode by verification keys using the settlement center 1 at the time of a commercial transaction for accounts to be settled even when the signature key has included a third party's hand, the degree of encryption of a signature key can also be weakened. Therefore, when enciphering a signature key, the password A can perform, and the password B can be made unnecessary.
[0029]
[Effect of the Invention]As explained above, according to this invention, a center and a terminal are connected via a network, When transmitting and registering with a center from the terminal side by making information, including personal information etc., into wording of a telegram, sign personal information in an individual by the terminal side, transmit to a center, and. Since it enciphers with a password and was made to keep this signature key, the high security nature of the personal information registered via a network can be secured, therefore the unauthorized use by the third party of such personal information can be prevented exactly. Since a password is managed only individually, the unauthorized use of a password is restricted when the person himself/herself involves by leak by the inattention of the person himself/herself, etc., and it can maintain security high as the whole system. Constitute the above-mentioned password from the 1st and 2nd passwords, and a terminal enciphers a signature key with the 1st password, and. Since it enciphers with the 2nd password further and the signature key enciphered with the 1st password was held, Even if the 1st password is decoded by the third party, since the signature key is further enciphered with the 2nd password, when a signature key is limited to use of only the person himself/herself and it, as a result, conducts the dealings of evidence by an electronic

signature, high security nature can be secured. When transmitting signature wording of a telegram to a center, encipher with the 1st password, save a terminal temporarily, and. Since are at the transmitting-in center time, it enciphers and transmits with a common key after decrypting this signature wording of a telegram with the 1st password, and this signature wording of a telegram is decrypted with a common key in the center and it was made to register, when registering personal information into a center, higher security nature can be secured. Since the center verified this signature wording of a telegram by the registered verification keys when the wording of a telegram signed by the signature key from the terminal was transmitted after registration of the above-mentioned personal information, In the center, when it can be checked whether this wording of a telegram is signed truly and, as a result, conducts the dealings of evidence by an electronic signature, high security nature can be secured.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention]This invention relates to the registration method of the information at the time of registering information, including personal information etc., via a network.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art]Electronic commerce technology (electronic commerce) is being realized by progress of multimedia art or the spread of the Internet. The payment system by a credit card is known as one of the payment systems on such a network.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention]As explained above, in this invention, a center and a terminal are connected via a network, When transmitting and registering with a center from the terminal side by making information, including personal information etc., into wording of a telegram, signed personal information in the individual by the terminal side, and it transmitted to the center, and it enciphers with a password and was made to keep this signature key.
Therefore, the high security nature of the personal information registered via a network can be secured, therefore the unauthorized use by the third party of such personal information can be prevented exactly.
Since a password is managed only individually, the unauthorized use of a password is restricted when the person himself/herself involves by leak by the inattention of the person himself/herself, etc., and it can maintain security high as the whole system. Constitute the above-mentioned password from the 1st and 2nd passwords, and a terminal enciphers a signature key with the 1st password, and. Since it enciphers with the 2nd password further and the signature key enciphered with the 1st password was held, Even if the 1st password is decoded by the third party, since the signature key is further enciphered with the 2nd password, when a signature key is limited to use of only the person himself/herself and it, as a result, conducts the dealings of evidence by an electronic signature, high security nature can be secured. When transmitting signature wording of a telegram to a center, encipher with the 1st password, save a terminal temporarily, and. Since are at the transmitting-in center time, it enciphers and transmits with a common key after decrypting this signature wording of a telegram with the 1st password, and this signature wording of a telegram is decrypted with a common key in the center and it was made to register, when registering personal information into a center, higher security nature can be secured. Since the center verified this signature wording of a telegram by the registered verification keys when the wording of a telegram signed by the signature key from the terminal was transmitted after registration of the above-mentioned personal information, In the center, when it can be checked whether this wording of a telegram is signed truly and, as a result, conducts the dealings of evidence by an electronic signature, high security nature can be secured.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]It is necessary to register personal information into a center via a network in such a settlement system. However, since such a settlement system intervenes networks, such as the Internet, and electronic commerce technology is performed between many and unspecified persons, there is a possibility that personal information may be freely used for others and unjust dealings may be conducted to them --- therefore, encoding technology and the person himself/herself --- it is requested that thoroughgoing organization is taken about security, such as attestation. Therefore, an object of this invention is to secure high security, when registering information, including personal information etc., via a network, and when holding personal information.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem]In order to solve such a technical problem, a center and a terminal are connected to this invention via a network, When transmitting to a center as wording of a telegram and registering information on a terminal via a network, a terminal, Sign with verification keys and the 2nd key (signature key) generated by pair to the above-mentioned wording of a telegram which consists of the 1st key (verification keys) for performing verification of the above-mentioned information and this information, transmit to a center, and make it register via a network, and. It is the method which enciphers with a password and held a signature key at a terminal. Therefore, when transmitting and registering with a center from the terminal side by making information, including personal information etc., into wording of a telegram, sign personal information in an individual by the terminal side, transmit to a center, and. Since it enciphers with a password and was made to keep this signature key, the high security nature of personal information registered via a network can be secured, therefore an unauthorized use by a third party of such personal information can be prevented exactly. Since a password is managed only individually, an unauthorized use of a password is restricted when the person himself/herself involves by leak by inattention of the person himself/herself, etc., and it can maintain security high as the whole system. Constituting the above-mentioned password from the 1st and 2nd passwords, a terminal enciphers a signature key with the 1st password (password B), and it is the method which enciphers with the 2nd password (password A) further, and held a signature key enciphered with the 1st password. Therefore, even if the 1st password is decoded by third party, since a signature key is further enciphered with the 2nd password, when a signature key is limited to use of only the person himself/herself and it, as a result, conducts dealings of evidence by an electronic signature, high security nature can be secured. When transmitting signature wording of a telegram to a center, encipher with the 1st password, save a terminal temporarily, and. It is at the transmitting-in center time, and after decrypting this signature wording of a telegram with the 1st password, it is the method registered after having enciphered with a common key (the 3rd key) generated temporarily, transmitting between centers and decrypting this signature wording of a telegram with a common key in the center. Therefore, when registering personal information into a center, higher security nature can be secured. When wording of a telegram signed by a signature key from a terminal is transmitted after registration of the above-mentioned information, a center is the method which verified this signature wording of a telegram by registered verification keys. Therefore, in the center, when it can be checked whether this wording of a telegram is signed truly by verification keys registered and, as a result, conducts dealings of evidence by an electronic signature, high security nature can be secured.
[0005]
[Embodiment of the Invention]Hereafter, this invention is explained with reference to drawings. Drawing 1 is a block diagram showing the composition of the system which applied this invention. In the figure, the center apparatus of the credit company 6 and 7A of networks, such as the Internet, the terminal (the following, common member's terminal) which a settlement center owns 1, 4A owns 3, and, as for 4B, a general member owns, the terminal (henceforth, store member's terminal) which, as for 5A and 5B, a store member owns, and 6A are the center apparatus of the

bank 7.
[0006]That is, the common member's terminals 4A and 4B are connected to the store member's terminals 5A and 5B via the network 3, and the settlement center 1 is connected to the network 3 via the dedicated line L1 or L2. It is connected to the center apparatus 6A of a credit company via the DDX circuit L3, and the settlement center 1 is connected to the center apparatus 7A of a bank via the dedicated line L4.
[0007]By the way, there are goods (later delivered goods) which are the existing mail order gestalten and are sold as goods displayed by the store member's terminal 5 which is a seller, goods, such as a document sold on that spot, software, and a picture, and goods, such as a game which employs a computer in real time. On the other hand, the general member who is a buyer transferred specified amount, for example to the bank account of the settlement center 1, etc. beforehand, and when this is checked by the settlement center 1, he acquires the virtual prepaid card in which the value information of the specified amount published from the settlement center 1 was given. If the goods which are provided via the network 3 from the store member's terminal 5, and are displayed on the terminal 4 here are purchased by the general member, In the settlement center 1, the price of purchasing commodities is subtracted from the value information of the virtual prepaid card given to the general member, and payment of the remuneration of the purchasing commodity is made to an applicable store member.
[0008]Next, drawing 2 is a block diagram showing the composition of the settlement center 1. The WWW server with which 12 delivers between the networks 3 and receives various kinds of information via the circuit selected with the router 11 in the figure, The security server which serves to prevent unjust access of as opposed to the settlement center 1 from the network 3 in 13, The communications server with which 14 performs the credit company 6 or the bank 7, and data communications, The communication processing server with which 15 performs a below-mentioned electronic signature, signature verification, etc. to creation of transmitted wording of a telegram (send data), the analyses of a received message (received data), and these wording of a telegram, The database with which 16 accumulates these processing information, and 17 are printers which output the output and log information of the error information generated in the settlement center 1 at the time of data processing.
[0009]18 is a settling server and the settling server 18, Perform storage and file management to the databases 19, such as registers, such as a member register (general member register), a store register, a signature key that is needed in the case of the above-mentioned encryption or an electronic signature, and verification keys, and a treating number register, and. If the received data from the communications server 15 are inputted, settlement processing of the virtual prepaid card published to each general member based on the memory content of the database 19 will be performed, and it gives the communication processing server 15 by using the processing result as send data. 20 is a server for reference / statistics which performs search and inquiry processing, a member's registration processing, refund processing, statistical-materials creation processing, etc., and is outputted to the printer 21. 23 is a backup center which backs up the information processed in the above each part.
[0010]Next, order is concretely explained for the processing operation of each part of this system later on using each drawing after drawing 3. It explains from the subscription processing of the member to this system first. Drawing 3 is a figure showing a general member's subscription processing to this system. In the settlement center 1, the initial screen format for a general member subscription application is always transmitted on the network 3 (time **). Here, if the user of the network 3 who inputted the initial screen format performs a subscription request from the terminal 4 (time **), in the settlement center 1, a subscription screen will be created and it will send to the terminal 4 (time **). If the above-mentioned user who inputted this subscription screen makes a subscription application from the terminal 4 (time **), in the settlement center 1, the application software for admission recognition (henceforth, AP software) which used the code function etc. will be prepared, and a user will download that AP software to the terminal 4 (time **). Then, general membership number use agreement etc. are mailed to the subscription proposer who is the above-mentioned user in the settlement center 1 (time **), membership registration data a subscription proposer checks this, use AP software

from the terminal 4, and using the code — transmitting (time **) — in the settlement center 1, it registers with the database 19 as a member register. Thus, subscription of the general member who is a buyer of goods is performed.

[0011]Next, a store member's subscription is performed in the procedure shown in drawing 4. That is, if the user of the network 3 who inputted the initial screen format from the settlement center 1 to the initial screen format for a store member affiliation application (time **) transmitted on the network 3 performs a subscription request from the terminal 5 (time **), in the settlement center 1, a subscription screen will be created and it will send to the terminal 5 (time **). If the above-mentioned user who inputted this subscription screen makes a subscription application from the terminal 5 (time **), in the settlement center 1, AP software for affiliation recognition which used the code function etc. will be prepared, and a user will download that AP software to the terminal 5 (time **). Then, in the settlement center 1, a store membership number member's store article etc. are mailed to the affiliation proposer who is the above-mentioned user (time **), store registration data an affiliation proposer checks this and using the code using the terminal 5 to AP software — transmitting (time **) — in the settlement center 1, it registers with the database 19 as a store member register. Thus, affiliation of the store member who is a seller of goods is performed.

[0012]In this way, after each member joins this system, a general member transmits the virtual prepaid card requested data using a below-mentioned electronic signature, a code, etc. to the settlement center 1 via the network 3 from the terminal 4, as shown in drawing 5 (time **). Then, in the settlement center 1, the payment from the general member is checked and the virtual prepaid card of the value information of the specified amount using an electronic signature, a code, etc. is published to the addressing to a general member (time **). A general member acquires the virtual prepaid card via the network 3 by time **.

[0013]Drawing 12 - drawing 15 are the figures showing the example of issue of such a virtual prepaid card by the settlement center 1. That is, in the example of drawing 12, a general member performs a prepaid demand using the terminal 4 first (time **). By then, the thing for which the virtual prepaid card which gave the value information of specified amount to that general member will be published if the credit data about this general member are asked to the credit company 6 in the settlement center 1 and credit data are acquired (time **). The general member who performed the prepaid demand acquires a prepaid card (time **). Then, in the settlement center 1, the specified amount is paid in from the credit company 6 (time **), and specified amount is pulled down from the account of the above-mentioned general member of the bank 7 in the credit company 6 (time **).

[0014]next — in the example of drawing 13, a general member uses the terminal 4 first — a prepaid demand — carrying out (time **) — transfer of the specified amount to the bank 72 or the post office 82 with the settlement center 1 and dealings is directed to the bank 71 or the post office 81 which has an own account via a circuit (time **). Then, transfer of specified amount is performed by the bank 71 or the post office 81 at the bank 72 or the post office 82 with the settlement center 1 and dealings (time **). In the settlement center 1, if the payment from the above-mentioned member who gave the prepaid demand to the bank 72 or the post office 82 is checked and payment is checked (time **), the virtual prepaid card of specified amount will be published to the above-mentioned addressing to a member. As a result, the general member who performed the prepaid demand acquires a prepaid card (time **).

[0015]next — in the example of drawing 14, a general member uses the terminal 4 first — a prepaid demand — carrying out (time **) — the specified amount to the bank 7 or the post office 8 with the settlement center 1 and dealings is transferred (time **). Then, in the settlement center 1, if the payment from the above-mentioned member who gave the prepaid demand to the bank 7 or the post office 8 is checked and payment is checked (time **), the virtual prepaid card of specified amount will be published to the above-mentioned addressing to a member. As a result, the general member who performed the prepaid demand acquires a prepaid card (time **).

[0016]next — in the example of drawing 15, a general member uses the terminal 4 first — a prepaid demand — carrying out (time **) — registered mail is mailed to the settlement center 1

(time **). Then, in the settlement center 1, if the registered mail from the above-mentioned member who performed the prepaid demand is received and payment is checked (time **), the virtual prepaid card of specified amount will be published to the above-mentioned addressing to a member. As a result, the general member who performed the prepaid demand acquires a prepaid card (time **).

[0017]In this way, if the virtual prepaid card in which value information was given is acquired, as shown in drawing 6, a general member, Operate the terminal 4, choose which goods to purchase among each goods which are provided via the network 3 from the store member's terminal 5, and are displayed on the terminal 4 (time **), order-taking-and-order-placement processing is made to complete (time **), and the price balancing account is directed to the settlement center 1 (time **). Then, processing of transactions as shown below between the common member's terminal 4 and the store member's terminal 5 is started.

[0018]That is, as shown in drawing 7, the demand information (payment indication), including a transaction number etc., that the electronic signature and the code were given is first sent to the settlement center 1 via the network 3 from the terminal 4 in this case (time **). In then, the settlement center 1 That member who performed this transaction number demand is general member check-top, demand information (advice of payment), including the transaction number etc. which performed the general member's balance attestation (time **), and gave the electronic signature and the code to the terminal 5 via the network 3, -- transmitting (time **) -- new remainder is notified to the terminal 4 (time **). As a result, settlement of accounts of a general member and a store member is completed.

[0019]Thus, after dealing of goods and settlement processing are performed, delivery of selling merchandise is performed to the common member's terminal 4 via the network 3 from the store member's terminal 5 (drawing 8). As a class of the goods delivered via the network 3 here, there are goods mentioned above, such as a document, software, and a picture, and the product of the existing mail order gestalt is delivered later. And after delivery of selling merchandise is performed, as shown in drawing 9, the application for payment of the price which is equivalent to the selling merchandise from the store member's terminal 5 to the settlement center 1 is transmitted (time **). Then, in the settlement center 1, this price amount equivalent is transferred to the account of the applicable store member of the bank 7 (time **).

[0020]Thus, as for this system, the buyer of goods purchases a virtual prepaid card from the settlement center 1 by the means of a credit card or a home banking, The seller of goods reduces a buyer's virtual balance by a commodity price via the settlement center 1 in electronic commerce technology, and performs invoicing to the settlement center 1, and used to be made to receive payment, while performing electronic commerce technology.

[0021]Drawing 10 is a flow chart in which showing important section operation of this invention, and showing the operation situation of each terminals 4 and 5 in the case of holding membership registration from each terminals 4 and 5 to the settlement center 1, and can secure security nature high as a system by stepping on each step as shown in drawing 10. That is, at Step S1, they are the two passwords A for encryption (the 1st password and the password B (the 2nd password) are entered.) first. Then, in Step S2, alter operation of the contents of registration to the settlement center 1 is performed. As these contents of registration, personal information, such as a member individual's address, a name, and a date of birth, is included. And the "kind" for generating the verification keys (public key) which become a signature key for verifying a below-mentioned signature key (secret key; equivalent to a seal) and this signature key at Step S3 continuously and a pair is inputted. When inputting this "kind" here, the sign by a member individual's autograph is inputted from the keyboard which the terminal 4 does not illustrate, for example, or it is automatically inputted using a random number within the terminal 4. Then, in step S4, the signature key and verification keys according to the inputted "kind" are generated. Here, when generating a signature key and verification keys, it is generated so that the function of a signature key may serve as verification keys. That is, when a signature key is set to p and q as an example, the verification keys n are generated so that it may be set to $n=p^2xq$.

[0022]The generated signature key is saved at the file which is not illustrated in each terminals 4

and 5, respectively. When saving a signature key here at a file, a signature key is enciphered with the password B at Step S5, it enciphers with the password A further with that individual's hysteresis information (namely, in this case individual merchandise purchase hysteresis information), and this is saved at a file. As a result, a signature key is kept by the file by a layered structure as shown in drawing 10 (a). Therefore, it is only that the third party can display the merchandise purchase hysteresis information of the individual applicable to the password A, etc. on the indicator which a terminal does not illustrate even if the password A is decoded by the third party, The signature key can secure high security nature, when it is not used for the act (service to be signed) accompanied by settlement of the merchandise purchase by a third party, etc. and, as a result, conducts the dealings of evidence by an electronic signature, since it is further enciphered with the password B.

[0023]Next, when registering an above-mentioned entry content to the settlement center 1, there are two kinds of following methods. First, the 1st method signs with a signature key at Step S6 to the contents inputted at Step S2, and the verification keys generated by step S4, enciphers this with the password A, and once saves it at a file. Subsequently, after solving a code with the password A at Step S7 (decryption), the settlement center 1 and a line connection are performed at Step S8. And after that, it enciphers with the common key (encryption key) temporarily generated by step S9 in the case of transmission of the contents of registration with the settlement center 1, and transmits to the settlement center 1. In the settlement center 1, this wording of a telegram is decrypted with the above-mentioned common key, and is registered. Next, the 2nd method performs the settlement center 1 and a line connection at Step S8, after signing with a signature key at Step S10 to the contents inputted at Step S2, and the verification keys generated by step S4. And after that, it enciphers with the common key (encryption key) temporarily generated by step S9 in the case of transmission of the contents of registration with the settlement center 1, and transmits to the settlement center 1. In the settlement center 1, this wording of a telegram is decrypted with the above-mentioned common key, and is registered.

[0024]Thus, it registers with the settlement center 1 with a gestalt as the personal data of a general member or a store member show to drawing 10 (b). Then, since it verifies whether the electronic signature of the wording of a telegram is carried out truly by the signature key and a pair of verification keys so that it may mention later when the wording of a telegram signed by the signature key from each terminal has been sent, in a commodity transaction, a reliable system is realizable in the settlement center 1.

[0025]Drawing 11 is a flow chart showing operation in case a general member's terminal 4 registered into the settlement center 1 in this way performs electronic commerce technology. Namely, if alter operation of the password A is performed at Step S11 in the settlement center 1 and the common member's terminal 4 in a non-connected state (offline state), The past transaction data (namely, shopping historical data; merchandise purchase hysteresis information) saved at the common member's terminal 4 is displayed on the indicator which the terminal 4 does not illustrate as an indicative data shown in drawing 11 (a) at Step S12. In drawing 11 (a), yy, mm, and dd show a year, the moon, and a day respectively.

[0026]Then, when alter operation of the password B is performed at Step S13 in the above-mentioned general member's terminal 4, in this member's terminal 4. It is judged as that from which the signature key for signing the wording of a telegram (namely, transaction number requested data described, for example by explanation of drawing 7) transmitted to the settlement center 1 was taken out, and a signature shifts to required service between the settlement centers 1 in Step S14. Namely, after a signature key is taken out by the input of the above-mentioned password B and the settlement center 1 and a line connection are performed, supposing the above-mentioned wording of a telegram is signed with that signature key and this signature wording of a telegram is transmitted from that common member's terminal 4, In the settlement center 1, this wording of a telegram is received, and this received message is decoded by the verification keys registered at the time of membership registration, and it checks. And if a check is set to O.K., after performing the general member's balance attestation, the advice of payment which gave the electronic signature and the code to the store member's

terminal 5 will be transmitted, and new remainder is notified to the common member's terminal 4.

[0027]Thus, in order to encipher the signature key certainly used with the passwords A and B at the clearing time, Even when the password A was decoded and a third party understands the whereabouts of a signature key, the third party cannot take out a signature key, therefore can prevent use of the signature key by a third party. That is, in this case, the third party can only peruse for example, the shopping history of the owner of this signature key, etc., and can prevent the shift to account settlement services to be signed. Since a signature key cannot be taken out unless the password A comes to hand, even if it can also expect the effect of being hard to use a signature key and the password B comes to hand by chance, even if a third party obtains a signature key by chance, the effect which prevents use of the password B is also expectable.
[0028]By providing a signature key and verification keys in a pair, managing a signature key at each terminal, putting verification keys in block in the settlement center 1, and managing, Since the third party has to make wording of a telegram certainly decode by verification keys using the settlement center 1 at the time of a commercial transaction for accounts to be settled even when the signature key has included a third party's hand, the degree of encryption of a signature key can also be weakened. Therefore, when enciphering a signature key, the password A can perform, and the password B can be made unnecessary.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the system of this invention.
[Drawing 2]It is a block diagram of the settlement center which constitutes the above-mentioned system.
[Drawing 3]It is a figure showing a general member's register operation.
[Drawing 4]It is a figure showing a store member's register operation.
[Drawing 5]It is a figure showing the virtual prepaid card acquisition operation through a common member's terminal.
[Drawing 6]It is a figure showing the selection operation of a purchasing commodity and order-taking-and-order-placement operation through a common member's terminal.
[Drawing 7]It is a figure showing the settlement-of-accounts operation at the time of a commodity transaction.
[Drawing 8]It is a figure showing the goods delivery situation at the time of a commodity transaction.
[Drawing 9]It is a figure showing payment operation of the settlement center at the time of a commodity transaction.
[Drawing 10]It is a flow chart showing an operation situation in case each terminal holds membership registration to a settlement center.
[Drawing 11]It is a flow chart showing operation in case a common member's terminal performs electronic commerce technology.
[Drawing 12]It is a figure showing the 1st example of virtual prepaid card acquisition.
[Drawing 13]It is a figure showing the 2nd example of virtual prepaid card acquisition.
[Drawing 14]It is a figure showing the 3rd example of virtual prepaid card acquisition.
[Drawing 15]It is a figure showing the 4th example of virtual prepaid card acquisition.
[Description of Notations]
1 -- A settlement center, 3 -- A network, 4, 4A, 4B -- Common member's terminal, 5, 5A, 5B -- A store member's terminal, 6 -- A credit company, 7 and 71, and 72 -- bank, 8 and 81, and 82 -- [-- A router, 12-15, 17, 18 20 / -- A server, 23 / -- Backup center.] A post office, 6A, 7A, 8A -- A center apparatus, 11, 22

[Translation done.]